

if the MAC ID is determined to be valid, determining if the identifier is valid;”

In the Office Action dated December 14, 2006, the Examiner admits that:

“Schuster et al. do not disclose explicitly receiving an identifier from the IP telephone; determining if a MAC ID for the IP telephone is valid; if the MAC ID is determined to be valid, determining if the identifier is valid.”

In the examiner’s Response to Argument, the examiner states:

“Examiner contends references Fijolek et al. disclose determining if a MAC ID for the IP phone is valid; if the MAC ID is determined to be valid, determining if the identifier is valid (see column 21, lines 12 – 30, lines 50-55; column 24, lines 49-49-60 (*sic*). Lee et al. teach determining if a MAC ID for the IP phone is valid; if the MAC ID is determined to be valid, determining if the identifier is valid (see column 1, lines 39-42.”

Applicant examines each of the above cited disclosures in turn below. The first disclosure cited by the examiner is column 21, lines 12-30, of Fijolek, reproduced below:

“CMTS 12 stores a pair of network address values in the ARP table, the IP 54 address of the selected network host interface from the DHCP 66 yiaddr-field 126 and a Network Point of Attachment ("NPA") address. In one preferred embodiment of the present invention, The NPA address is a MAC 44 layer address for the CM 16 via a downstream cable channel. The IP/NPA address pair are stored in local routing tables with the IP/NPA addresses of hosts (e.g., the CMs 16) that are attached to cable network 14.

At Step 210, the CMTS 12 sends the DHCPACK message to the CM 16 via the cable network 14. At Step 212, the CM 16 receives the DHCPACK message, and along with the CMTS 12 has addresses for a "virtual connection" between the data network 28 and the CM 16. When data packets arrive on the IP 54 address for the selected CM 16 they are sent to the CMTS 12 and the CMTS 12 forwards them using a NPA (i.e., a MAC 44 address) from the routing tables on a downstream channel via the cable network 14 to the CM 16.”

As can be seen, this disclosure of Fijolek merely describes the CMTS (cable modem termination system) may store IP/NPA address pairs in an ARP table. This disclosure also describes the CMTS may forward messages using the NPA (e.g., a MAC address). However, nothing in this disclosure teaches or suggests “determining if a MAC ID for the CM is valid; if the MAC ID is determined to be valid” as suggested by the examiner.

The second disclosure cited by the examiner is column 21, lines 50-55, reproduced below:

“After Method 188, the CMTS 12 has a valid IP/MAC address pair in one or more address routing tables including an ARP table to forward IP 54 data packets from data network 28 to the CM 16, thereby creating a virtual IP 54 data path to/from the CM 16 as was illustrated in and Table 3.”

While the above disclosure mentions a “valid IP/MAC address pair”, there is in fact no disclosure in Fijolek of “determining if a MAC ID for the IP phone is valid; if the MAC ID is determined to be valid, determining if the identifier is valid” as recited. The description and context of the above disclosure is found in col. 18, line 60 – col. 22, line 44 of Fijolek. Upon review of this disclosure it is found that an entity (CM) conveys a DHCP Request message which includes a field for storage of a MAC address (see Table 8, CHADDR 132, of Fijolek). During the described process, the CMTS stores a pair of network address values in the ARP table. The first value comes from the yiaddr-field 126 of the DHCP 66, and the second value is an NPA address which is in one embodiment a MAC address - the value that was conveyed in the CHADDR 132 field of the DHCP Request message. As disclosed in Fijolek, “CMTS 12 updates an Address Resolution Protocol (“ARP”) table and other routing tables on the CMTS 12 to reflect the addresses in the DHCP 66 yiaddr-field 126 and the DHCP 66 chaddr-field 132 at Step 208.” This is the “valid IP/MAC address pair” mentioned in the above disclosure. However, while the word “valid” appears in the disclosure above, nowhere is there any disclosure in Fijolek of determining if a MAC ID is valid as recited.

The third disclosure cited by the examiner is column 24, lines 49-60 of Fijolek, reproduced below:

“At Step 314, the CMTS 12 receives the DHCPACK message. the CMTS 12 examines the DHCP 66 giaddr-field 130 and looks up that IP 54 address in its ARP table or other routing tables for an associated MAC 44 address. This is a MAC 44 address for the CM 16, which sent the DHCPREQUEST message from CPE 18. The CMTS 12 uses the MAC 44 address associated with the DHCP 66 giaddr-field 130 and the DHCP 66 yiaddr- field 126 to update its routing and ARP tables reflecting this address pairing at Step 316. At Step 318, the CMTS 12 sends the DHCPACK message on a downstream channel on cable network 14 to the IP 54 and MAC 44 addresses, respectively (i.e., to the CM 16).”

Here again, the disclosure simply states the MAC address that was received in an earlier request message is assumed valid and used as such. However, there is nothing concerning the above recited features disclosed herein.

The fourth disclosure cited by the examiner is column 1, lines 39-42, of Lee, reproduced below:

“According to an aspect of the present invention, there is provided a method and apparatus for registering IP phones with an IP phone switch using access codes or personal identification numbers for authentication and for associating directory numbers to MAC addresses of IP phones.”

As per the reference Lee, in the Office Action the examiner also states:

“Lee et al. disclose the limitation of receiving an identifier from the IP telephone (recited “IP phone then sends a request for registration to the IP phone service provider, which includes its MAC address and set type” as an identifier from the IP telephone; column 3, lines 16 - 32, Fig. 3, element 318, Reg Device (MAC, IP

address, Set Type); determining if a MAC ID for the IP telephone is valid (recited "upon receipt of the validation request" as determining if a MAC ID for the IP telephone is valid; column 3, lines 44 - 45, Fig. 3, elements 334 Validate PIN(MAC,PIN)); if the MAC ID is determined to be valid, determining if the identifier is valid (recited "the access code is then validated" as the MAC ID is determined to be valid, and "Valid PIN" as determining if the identifier is valid; column 3, lines 49 - 55, FIG. 3, element 336 Valid PIN(MAC))."

However, Applicant disagrees with the examiner's characterization as to what is disclosed by Lee. In contrast to the examiner's suggestions, Lee discloses the following:

"FIG. 3 shows a data flow for registration of an unregistered IP phone 102 on the IP phone switch 100 where a PIN has been assigned to a user, but a MAC address has not been associated with the PIN. The composition of the PIN includes an access code and a DN.

. . . The IP phone 102 then sends a request 318 for registration to the IP phone service provider 202, which includes its MAC address and set type. The IP phone service provider 202 then sends an Open Port request 320 with the MAC address, the set type, and the IP address (associated information) to the set registration process 204 for registration of the IP phone 102.

The set registration process 204 upon receiving the Open Port request 320 checks the information against its lookup table of data shared with OAM 206 as shown at 322. In the present example of an unregistered IP phone 102, as there is no match 324 for the MAC address, the set registration process 204 sends a message to request a PIN 326, 328 from the user of the IP phone 102. . . . Upon receipt of the PIN from the user, the IP phone sends the PIN 330 to the IP phone service provider 204, which then sends an Open Port PIN request 332 with the PIN and associated information to the set registration process 204. The set registration process 204 in turn sends a validation request 334 with the PIN and the MAC address to the OAM 206.

The OAM 206, upon receipt of the validation request 334, strips the access code and DN from the PIN. The access code is then validated. The association of the DN with the MAC address is set up in the OAM 206 for directing calls accordingly. Upon completion of the set up, the OAM 206 sends a message, Valid PIN 336, to the set registration process 204 indicating that the set is registered. The lookup table is then updated in both the OAM 206 and the set registration process 204.." (Lee, col. 3, lines 8-55).

As seen from the above, a user PIN includes an access code and a DN (directory number). The registration process 204 receives an Open Port request with MAC address, set type, and IP address from the IP phone service provider. If the IP phone is unregistered, there is currently no associated MAC address in the database. Therefore, the registration process sends a request for a PIN to the IP phone. The IP phone returns the PIN (the user PIN includes an access code and a DN (directory number)). The registration process then sends a validation request with the PIN and MAC address to the OAM (database). The OAM then strips the access code and DN from the PIN and validates the access code. The association between the DN and the MAC address is then set up in the OAM database. Note that there is no validation of the MAC address in Lee. In contrast, Lee teaches validating the access code. Should the access code be validated, the received MAC address is associated with the DN. Therefore, Lee does not disclose "determining if a MAC

ID for the IP telephone is valid as suggested. Rather, upon receipt of the validation request, the access code is validated – not the MAC address.

Further, Lee does not disclose “if the MAC ID is determined to be valid, determining if the identifier is valid. Rather, Lee discloses validating the access code and sending a Valid PIN message. Sending the valid PIN message is not a separate validation process. Rather, the valid PIN message is in response to validating the access code and completion of the set up.

As the combination of references do not disclose or suggest all the features of the claims as suggested, Applicant requests withdrawal of the rejections for at least the above reasons.

Applicant also notes new rejections have been raised in the Office Action dated December 14, 2006. In particular, 35 U.S.C. § 101 rejections have been raised, suggesting that claims 1-8, 10-15, 31-38, and 40-45 are directed to non-statutory subject matter. Applicant does not agree and believes the claims are *clearly* statutory. Also newly raised is an obviousness type double patenting rejection in view of a prior patent of the Applicant. Applicant also does not agree with this rejection. Nevertheless, in view of the clear errors noted above, and the limited space provided herein for the present Request, Applicant does not further address these newly raised issues at this time.

In light of the foregoing remarks, Applicant respectfully requests withdrawal of the above discussed rejections. If any extension of time (under 37 C.F.R. § 1.136) is necessary to prevent the above referenced application from becoming abandoned, Applicant hereby petitions for such an extension. If any fees are due, the Commissioner is authorized to charge said fees to Meyertons, Hood, Kivlin, Kowert & Goetzel PC Deposit Account No. 501505/5686-00300/RDR.

Respectfully submitted,

/ Rory D. Rankin /

Rory D. Rankin

Reg. No. 47,884

ATTORNEY FOR APPLICANT(S)

Meyertons, Hood, Kivlin, Kowert, & Goetzel, P.C.
P.O. Box 398
Austin, TX 78767-0398
Phone: (512) 853-8850

Date: June 13, 1007